Techno.COM, Vol. 18, No. 2, Mei 2019 : 110-121

Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital

Implementation of Rivest Shamir Adleman (RSA) Cryptography Algorithm On Digital Signatures

Yusuf Anshori[*1], A. Y. Erwin Dodu[2], Dewa Made P. Wedananta[3]
[1,2,3]Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Tadulako
Jl. Soekarno Hatta Km. 9, Palu, Sulawesi Tengah, Telp. (0451)422355, Fax. (0451) 454014
e-mail: [*1]iyus.jr@gmail.com, [2]ayerwin.dodu@gmail.com, [3]dewa.pramudia08@gmail.com

Abstrak

Tanda tangan digital merupakan mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Tanda tangan digital dapat digunakan untuk melakukan pembuktian secara matematis bahwa data tidak mengalamai modifikasi secara illegal, sehingga bisa digunakan sebagai salah satu solusi untuk melakukan verifikasi data. Penelitian ini bertujuan untuk menerapkan algoritma kriptografi Rivest Shamir Adleman (RSA) pada tanda tangan digital. Proses pembuatan tanda tangan digital diawali dengan pembuatan message digest dari sebuah dokumen kemudian proses pembangkitan kunci publik dan kunci privat untuk mengamankan data dan untuk membuat tanda tangan digital. Kunci privat akan dikirimkan kepada penerima pesan untuk memverifikasi tanda tangan digital. Tanda tangan digital dan dokumen dikirmkan kepada penerima. Selanjutnya, pada proses verifikasi, penerima akan mengecek apakah tanda tangan tersebut cocok atau tidak dengan menggunakan kunci privat dan menghitung nilai hash (message digest) dari dokumen yang diterima.

Kata Kunci — Tanda Tangan Digital, Algoritma Rivest Shamir Adleman (RSA), Fungsi Hash, Kriptografi

Abstract

A digital signature is an authentication mechanism that allows the message maker to add a code which acts as a signature. The digital signature can be used to mathematically prove that the data does not experience modification illegally, so that it can be used as a solution to verify data. This study aims to implement the Rivest Shamir Adleman (RSA) cryptographic algorithm in digital signatures. The process of making digital signatures begins with the creation of message digest from a document then the process of generating a public key and private key to secure data and to make a digital signature. A private key will be sent to the recipient of the message to verify the digital signature. The digital signature and document are sent to the recipient. The next step is the verification process which the recipient checks whether the signature is suitable or not by using the private key and calculates the hash (message digest) value of the document received.

Keywords— *Digital Signature, Rivest Shamir Adleman Algorithm (RSA), Hash Function, Cryptography*

1. PENDAHULUAN

Tanda tangan digital adalah sebuah teknik dalam kriptografi yang dapat digunakan untuk menandatangani dokumen digital. Tanda tangan digital juga merupakan hasil dari

diberlakukannya teknik kriptografi terhadap isi dokumen asli. Kriptografi bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan, seperti LAN atau internet, tidak dapat diketahui dan dimanfaatkan oleh orang lain atau pihak yang tidak berkepentingan [1]. Dokumen yang hendak dikirim terlebih dahulu dikenai fungsi *hash*sehingga menjadi bentuk yang ringkas yang disebut dengan *message digest*. Kemudian, *message digest* dienkripsi menggunakan algoritma kriptografi kunci-publik, kunci privatmilik penandatangan atau pengirim dokumen akan digunakan untuk melakukan enkripsi message digest. Hasil dari enkripsi inilah yang disebut sebagai tanda tangan digital (*digital signature*) [2].Tanda tangan digital harus memiliki fungsi yang sama dengan tanda tangan konvensional, yaitu dapat menjamin integrity, authenticity, dan non-repudiation. Tanda tangan digital dibangkitkan dari hash terhadap pesan. Nilai hash adalah kode ringkas dari pesan. Tanda tangan digital berlaku seperti tanda tangan dokumen kertas, tanda tangan digital ditambahkan (append) pada pesan [3]. Perbedaan utama antara tanda tangan konvensional dengan tanda tangan digital yaitu tanda tangan konvensional dapat disalin baik secara manual maupun dengan scan copy dan dapat digunakan secara berulang, sedangkan tanda tangan digital sangat bergantung kepada dokumen yang ditanda tangani, sehingga untuk setiap dokumen menghasilkan tanda tangan yang berbeda satu sama lain.

Dengan semakin berkembangnya teknologi dibidang internet, sebuah dokumen kini tidak hanya diterbitkan dalam bentuk cetak saja, tetapi juga dalam bentuk digital. Dokumen yang ditransmisikan melalui internet sangat rentan terhadap kemungkinan modifikasi serta sulitnya pembuktian keaslian dokumen tersebut. Pengirim dapat dengan mudahnya menyangkal bahwa dialah yang telah menulis atau mengirimkan dokumen tersebut. Tanda tangan digital menggunakan fungsi hash SHA3 dan algoritma kriptografi RSA dalam implementasinya agar dapat menjamin keaslian isi dokumen. Fungsi hash SHA3 untuk membentuk message digest dari sebuah dokumen dan algoritma kriptografi RSA digunakan untuk mengenkripsi message digest tersebut sehingga menghasilkan tanda tangan digital. Algoritma RSA adalah algoritma asimetris yaitu algoritma yang mempunyai dua kunci berbeda untuk proses enkripsi dan dekripsi yaitu kunci publik dan kunci privat [4].

Proses utama pada tanda tangan digital terdiri atas dua proses, yaitu proses signing (tanda tangan) dan verifikasi. Proses signing dilakukan dengan mengubah sebuah isi dokumen menjadi message digest dan mengenkripsinya menggunakan algoritma kriptografi RSA. Sementara, proses verifikasi dilakukan dengan membandingkan hasil dekripsi isi dokumen yang diterima (ciphertext) dengan message digest dari isi dokumen sebenarnya.

Algoritma Kriptografi dari setiap kriptografi klasik selalu terdiri dari dua bagian yaitu enkripsi dan dekripsi [5]. Algoritma kriptografi Rivest Shamir Adleman (RSA)adalah algoritma untuk enkripsi kunci publik (*public-key encryption*). Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandatangani (*signing*) dan untuk enkripsi (*encryption*) dan salah satu penemuan besar pertama dalam kriptografi kunci publik [6]. Algoritma ini tidak berdasarkan pada proses enkripsi dan dekripsi, melainkan lebih kepada proses matematika yang dilakukan untuk menghasilkan kunci rahasia yang dapat disebarkan secara bebas tanpa harus khawatir karena kunci rahasia tersebut hanya dapat didekripsi hanya oleh pengirim dan penerima pesan. Dasar dari algoritma ini memfaktorkan bilangan yang besar menjadi faktor-faktor prima [7].

Pada penelitian yang dilakukan Ginting *et al*, diperoleh fakta bahwa penggunaan algoritma kriptografi RSA untuk enkripsi dan dekripsi email dapat berjalan dengan baik karena pada aplikasi yang dikembangkan, satu pesan asli dapat menghasilkan *ciphertext* yang berbeda-beda, karena proses pembangkitan kunci RSA didasarkan oleh nilai *p* dan *q* yang acak. Hal ini mengakibatkan pesan akan sulit di dekripsi oleh orang lain sehingga memerlukan kunci privat dari pengirim pesan tersebut [8].

Mengamankan data sertifikat tanah digital yakni dengan menggunakan *digital signature* SHA-512 sebagai proses *hashing* bagian *xreftable* dari *file* pdf sertifikat, selanjutnya dienkripsi dengan Algoritma RSA menjadi *signature* kemudian disisipi ke sebuah dokumen sertifikat tanah digital. Hal ini akan mengakibatkan sistem pengamanan sertifikat tanah digital dapat

mengidentifikasi ada tidaknya perubahan yang terjadi pada *file* dokumen sertifikat digital sehinggadapat disimpulkan bahwa sistem dapat memverifikasi keaslian dari *file* dengan menggunakan SHA-512 dan RSA [9].

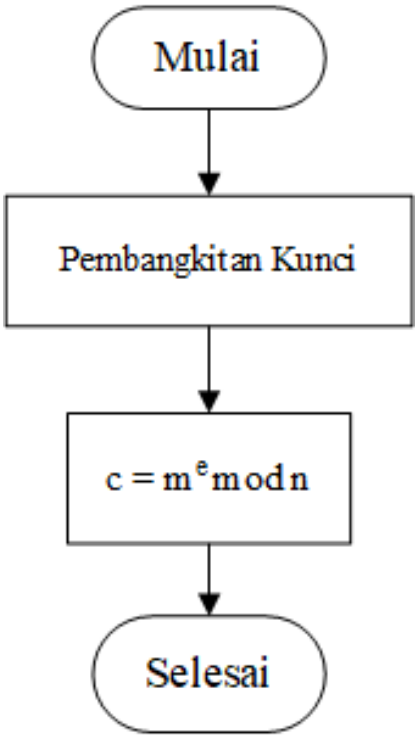
2. METODE PENELITIAN

2.1. Pengumpulan Data

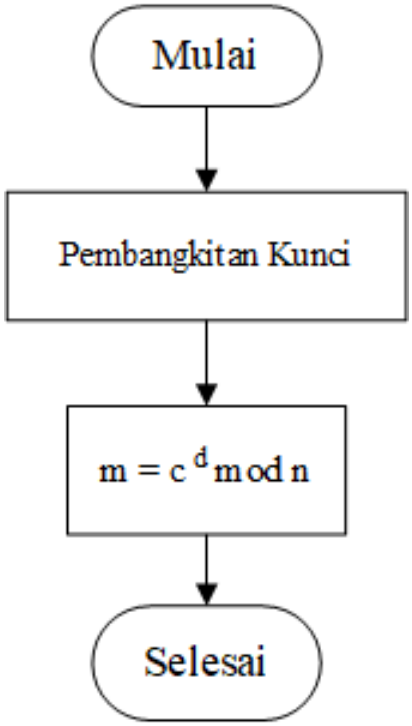
Melakukan pengumpulan data dari sumber yang berkaitan dengan perancangan system. Pengumpulan data melalui survei padatempat penelitian, data yang dikumpulkan adalah dokumen berformat (*txt*, *docx*, dan *pdf*). Data yang telah dikumpulkan kemudian dianalisis sesuai kebutuhan dalam melakukan perancangan serta pembentukan tanda tangan digital.

2.2. Perancangan Perangkat Lunak

Melakukan perancangan kebutuhan perangkat lunak dan tahapan-tahapan proses implementasi algoritma kriptografi RSA pada tanda tangan digital untuk menjalankan proses enkripsi, digunakan kunci public yang telah dibentuk sebelumnya, yaitu kunci publik (n, e). Sedangkan dalam proses dekripsi RSA digunakan kunci rahasia yang sudah ditentukan sejak awal perhitungan. Pasangan kunci rahasia (n, d) [10]. *Flowchart* enkripsi algoritma kriptografi RSA dan *flowchart* dekripsi algoritma kriptografi RSA dapat dilihat pada gambar 1, dan 2.



Gambar 1 *Flowchart* enkripsi algoritmakriptografi RSA.



Gambar 2 *Flowchart* dekripsi algoritma kriptografi RSA

2.3. Pembuatan Perangkat Lunak

Dalam melakukan pembuatan aplikasi ada beberapa tahap diantaranya : melakukan persiapan *software* yang digunakan, membuat desain *interface*, dan fungsi menu aplikasi.

Berikut ini adalah desain fungsi dari aplikasi yang dirancang :

1. Halaman *Login*

   Halaman *login* digunakan untuk masuk ke aplikasi, pengguna harus memasukkan username dan password yang sesuai pada *form* tersebut, halaman *login* juga digunakan agar mencegah pengguna yang menyalahgunakan aplikasi.
2. Halaman Enkripsi

   Halaman enkripsi bertujuan untuk melakukan pembentukan kunci dan proses enkripsi menggunakan algoritma kriptografi RSA sekaligus pembuatan tanda tangan digital yang diterapkan pada dokumen berformat (*txt*, *docx*, dan *pdf*).
3. Halaman Dekripsi

   Halaman dekripsi bertujuan untuk melakukan proses dekripsi pada *ciphertext* sekaligus proses verifikasi tanda tangan digital pada sebuah dokumen text apakah dokumen tersebut masih asli atau telah dimodifikasi.
4. Halaman Admin

   Halaman admin bertujuan untuk melakukan proses pendaftaran pengguna aplikasi, agar hanya pengguna terpercaya yang dapat menggunakan program tersebut serta tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.
5. Halaman Kunci

   Halaman kunci bertujuan untuk menyimpan nilai *n*, kunci *e* dan kunci *d*, yang telah digunakan pada saat proses enkripsi. Pada halaman ini, admin dapat melakukan pengiriman *file* dokumen beserta kunci kepada penerima dokumen, pengiriman dilakukan menggunakan email.

2.4. Pengujian Perangkat Lunak

Pada tahap ini dilakukan pengujian perangkat lunak secara menyeluruh untuk memastikan fungsi-fungsi dari perangkat lunak telah berjalan dengan baik sesuai yang diharapkan dengan memastikan tidak ada *bug* ataupun *logic error* pada aplikasi tanda tangan digital. Kemudian algortima RSA diuji melalui pembangkitan kunci publik dan kunci privat ini bertujuan agar nilai $p \neq q$ karena apabila nilai $p = q$, maka $n=p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n. Selanjutnya pengujian proses enkripsi , dekripsi dan proses verifikasi pada tahap terakhir.

3. HASIL DAN PEMBAHASAN

3.1 Analisa Sistem

Pada analisa system, aplikasi tanda tangan digital dapat melakukan beberapa hal yaitu :

1. Aplikasi dapat melakukan pembentukan tanda tangan digital dari sebuah dokumen.
2. Aplikasi dapat melakukan pembentukan kunci secara otomatis.
3. Aplikasi dapat menyimpan tanda tangan digital.
4. Aplikasi dapat melakukan verifikasi tanda tangan digital.
5. Aplikasi dapat mengirim kunci privat melalui *email*.

3.2. Pengujian Sistem

Pengujian sistem dilakukan untuk mengetahui apakah fungsi-fungsi yang terdapat dalam sistem berjalan dengan baik atau tidak. Pengujian dibagi menjadi 5 jenis pengujian yaitu :

1. Pengujian *Message Digest*

   Pada pembentukan *message digest*, fungsi hash SHA3 digunakan membentuk *message digest* dari dokumen yang diinputkan. Fungsi hash dalam kriptografi adalah fungsi hash yang berupa sebuah algoritma yang mengambil sejumlah blok data dan mengembalikan *bit string* berukuran tetap. Pada tabel 1. dapat dilihat bahwa berapapun ukuran *string* yang diinputkan hasil *message digest* tetap mengeluarkan ukuran *output* yang sama.

Tabel 1 Hasil percobaan pembentukan *message digest.*

Percobaan Ke -	String	*Message Digest*
1	saya	48344c5e46271c1f76866f81b6f3230249 159ac183eca3f53ff27cbc83b85248
2	dan	ecb975254c53623d2c8273332e6fda81 60a187b381279de20e624f4d1aec9c5d
3	*message*	7f4a23d90de90d100754f82d6c14073 b7fb466f76fd1f61b187b9f39c3ffd895
4	enkripsi dan dekripsi	b07ba8266a2f291693e604d0e2cde2ba 23f36b0afbda838a4d4ef89daeb5b0eb
5	12345678	39d1da1f4f9fda75ac2c0b29b76c2149f e57256e3240ce35e1e74d6b6d898222

2. Pengujian Pembangkitan Kunci Publik dan Kunci Privat

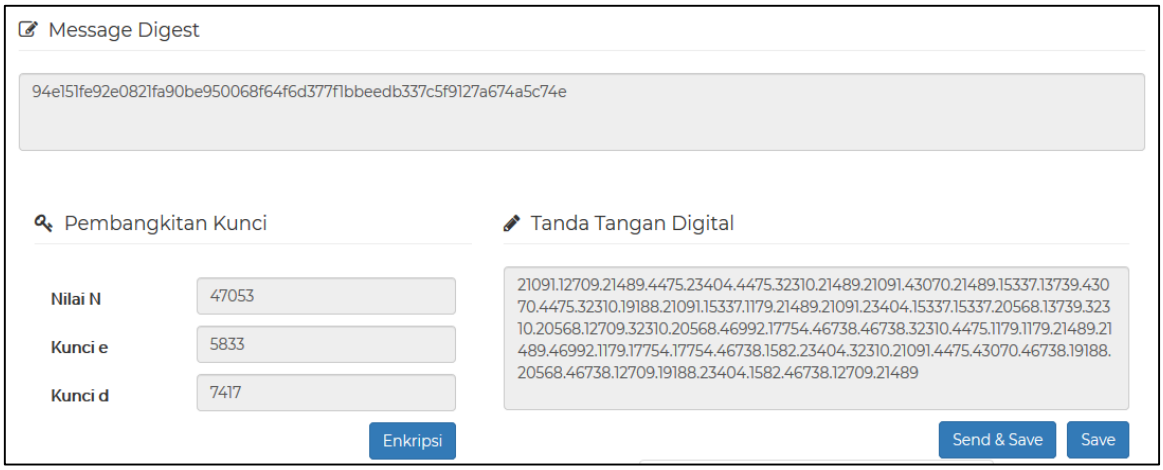
Dalam proses pembangkitan kunci, baik kunci publik maupun kunci privat pada algoritma kriptografi RSA, hal yang pertama dilakukan adalah pemilihan bilangan prima sembarang p dan q, nilai $p \neq q$ karena apabila nilai $p = q$, maka$n=p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n. Tabel 2. pengujian pembangkitan kunci publik dan privat dimana nilai p ≠ q.

Tabel 2 Pembentukan kunci publik dan kunci privat

Percobaan Ke -	P	q	n	e (Kunci Publik)	d (Kunci Privat)
1	761	1009	767849	4661	62621
2	587	577	338699	2873	105737
3	971	907	880697	3217	297493
4	541	809	437669	4477	57013
5	587	911	534757	3153	277877

3. Pengujian Proses Enkripsi Algoritma Kriptografi RSA

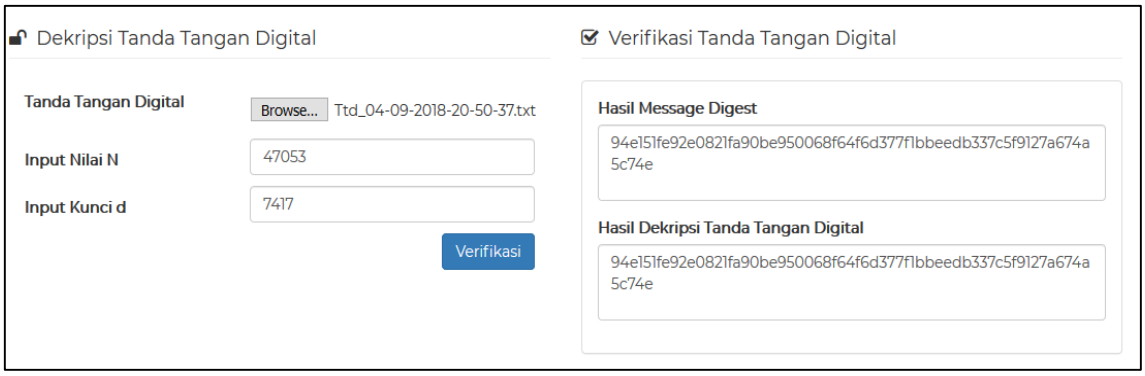
Pada proses enkripsi, *message digest* yang dihasilkan dari dokumen dienkripsi menggunakan algoritma kriptografi RSA menggunakan kunci publik yang telah didapat dari proses pembangkitan kunci sebelumnya. Hasil enkripsi inilah yang digunakan menjadi tanda tangan digital. Hasil tanda tangan digital dapat dilihat pada gambar 3.



Gambar 3 Hasil tanda tangan digital

4. Pengujian Proses Dekripsi Algoritma Kriptografi RSA

Pada proses dekripsi ini, penerima melakukan dekripsi pada tanda tangan digital dengan cara menginput nilai n, kunci d (kunci privat) dan tanda tangan digital lalu penerima melakukan dekripsi. Hasil dekripsi tanda tangan digital dapat dilihat pada gambar 4.



Gambar 4 Hasil dekripsi tanda tangan digital

5. Pengujian Verikasi Tanda Tangan Digital

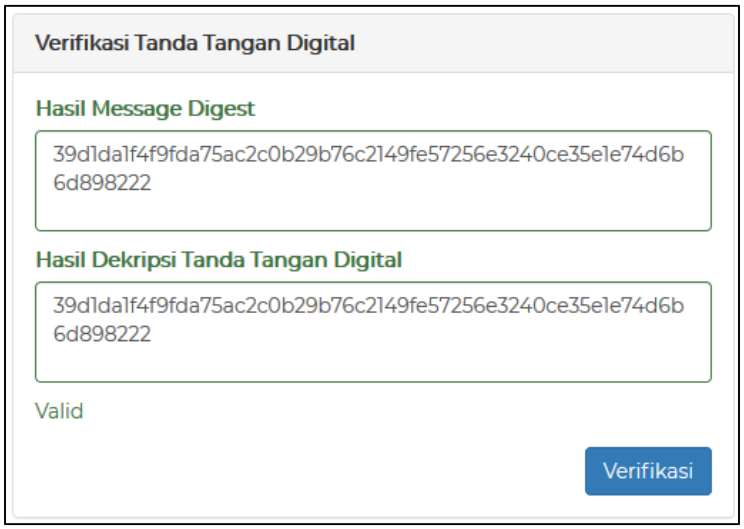
Pengujian verifikasi dilakukan untuk mengetahui apakah dokumen telah mengalami perubahan, penambahan atau pengurangan isi dari sebuah dokumen. Apabila hasil verifikasi valid maka dapat disimpulkan bahwa tidak adanya terjadi perubahan dokumen beserta tanda tangan digital. Sedangkan apabila hasil verifikasi tidak valid maka kemungkinan dokumen atau tanda tangan digital mengalami perubahan, penambahan ataupun pengurangan isi dokumen dan tanda tangan digital. Tabel 3. memperlihatkan hasil proses verifikasi dari beberapa kasus percobaan :

Tabel 3 Hasil verifikasi dari beberapa percobaan

Percobaan Ke -	Dokumen		Tanda Tangan Digital		d (Kunci Privat)		Hasil Verifikasi
	S	TS	S	TS	S	TS	
1	√	-	√	-	√	-	Valid
2	√	-	√	-	-	√	Tidak Valid
3	√	-	-	√	√	-	Tidak Valid
4	√	-	-	√	-	√	Tidak Valid
5	-	√	√	-	√	-	Tidak Valid
6	-	√	√	-	-	√	Tidak Valid
7	-	√	-	√	√	-	Tidak Valid
8	-	√	-	√	-	√	Tidak Valid

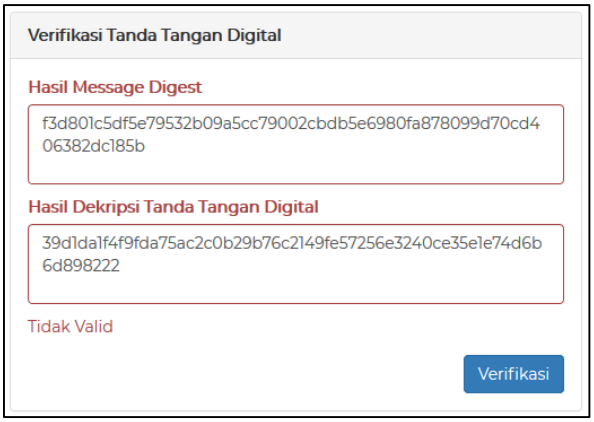
Keterangan : S = sah , TS = tidak sah , √ = ya.

Hasil verifikasi yang valid dimana hasil *message digest* memiliki *output* yang sama dengan hasil dekripsi tanda tangan digital dapat dilihat pada gambar 5.



Gambar 5 Tampilan hasil verifikasi valid

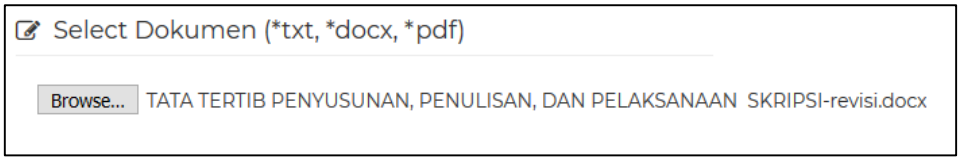
Sedangkan hasil verifikasi yang tidak valid karena memiliki *output* hasil *message digest* yang berbeda dengan *output* hasil dekripsi tanda tangan digital dapat dilihat pada gambar 6.



Gambar 6 Tampilan hasil verifikasi tidak valid

3.3. Pembuatan Tanda Tangan Digital

Tahap pertama dalam proses pembuatan tanda tangan digital yaitu menginputkan dokumen yang ditandatangani, kemudian pembuatan *message digest*, *message digest* didapatkan dengan cara melakukan generate isi dokumen yang telah diinputkan pada field pesan, kemudian dokumen tersebut dikenai fungsi hash SHA3, sehingga menghasilkan *message digest.* Proses *input* dokumen dapat dilihat pada gambar 7. dan hasil *message digest* dapat dilihat pada gambar 8.

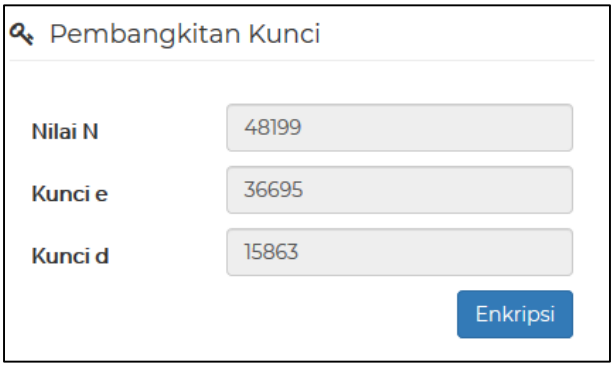


Gambar 7 Proses *input* dokumen berformat *docx*.

.

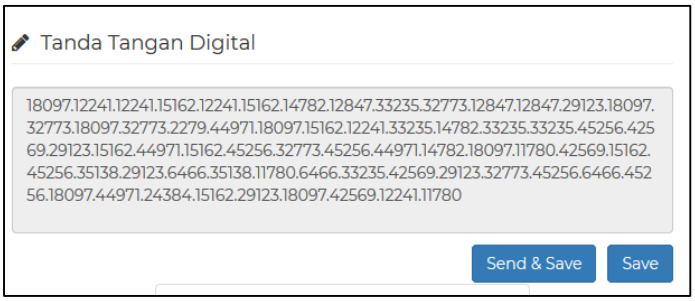
Gambar 8 Hasil *message digest* dokumen berformat *docx*.

Tahap selanjutnya adalah pembuatan kunci publik dan kunci privat, pada proses ini aplikasi melakukan pemilihan bilangan prima acak untuk nilai p dan q, nilai $p \neq q$ karena apabila nilai $p = q$, maka$n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n, selanjutnya algoritma *Euclidian* digunakan untuk mencari dua buah bilangan bulat yang relatif prima. Dua buah bilangan bulat dikatakan relatif prima jika GCD dari kedua bilangan bernilai = 1. Dimana nilai e (kunci publik) harus relativ prima terhadap ϕn, sehingga nilai GCD (ϕn , e) harus bernilai = 1. Kemudian hitung kunci d (kunci privat) dengan menggunakan persamaan $d = \frac{1+k\,\phi n}{e}$perhitungan nilai k menggunakan proses komputasi *looping* dengan mencoba nilai-nilai dimulai dari 1,2,3,dst sampai diperoleh nilai d berupa bilangan bulat. Hasil pembangkitan kunci publik dan kunci privat dapat dilihat pada gambar 9.



Gambar 9 Hasil pembentukan kunci publik dan kunci privat.

Setelah proses pembentukan kunci publik dan kunci privat selesai maka selanjutnya *message digest* dari dokumen dienkripsi menggunakan kunci publik hasil dari pembangkitan kunci sebelumnya. Hasil enkripsi inilah yang akan menjadi tanda tangan digital dari dokumen berformat *docx* yang telah diinputkan sebelumnya. Hasil tanda tangan digital dapat dilihat pada gambar 10.

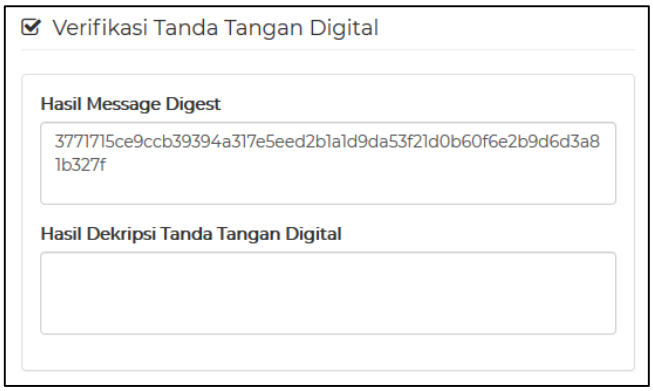


Gambar 10 Hasil tanda tangan digital dokumen berformat *docx*.

Kemudian dokumen, tanda tangan digital dan kunci privat dapat dikirim ke penerima dokumen, penerima dokumen melakukan verifikasi untuk mengetahui apakah dokumen dan tanda tangan digital masih terjaga keasliannya.

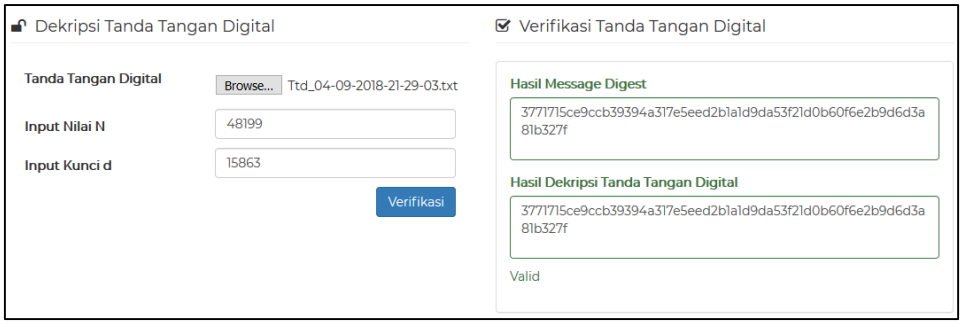
3.4. Proses Verifikasi Tanda Tangan Digital

Dalam melakukan verifikasi terdapat 3 tahapan, tahap pertama penerima menginput dokumen yang telah diberikan dalam hal ini dokumen berformat *docx*, dokumen diinput kedalam field pesan, kemudian digenerate menggunakan fungsi hash SHA3 sehingga menghasilkan *message digest*. Hasil *message digest* dapat dilihat pada gambar 11.



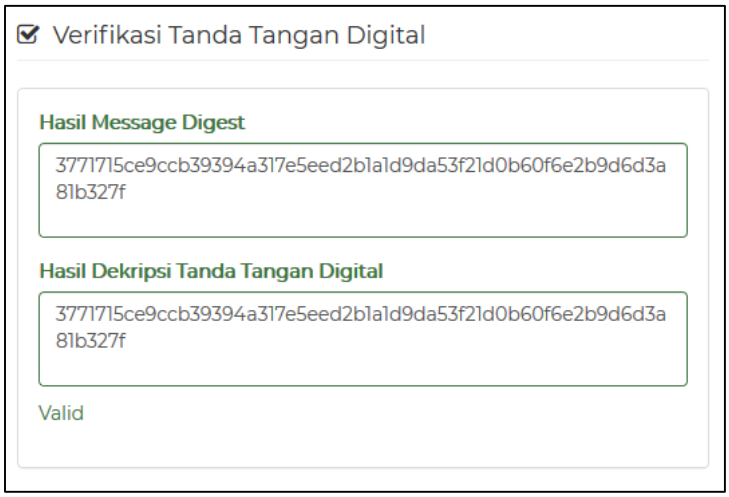
Gambar 11 Hasil *message digest* dari dokumen berformat *docx*.

Tahap kedua yaitu melakukan dekripsi tanda tangan digital, dekripsi dilakukan dengan cara menginputkan nilai *n*, kunci *d* (kunci privat) dan tanda tangan digital yang telah diterima dari pengirim. Proses dekripsi tanda tangan digital dapat dilihat pada gambar 12.



Gambar 12 Proses dekripsi tanda tangan digital

Tahap terakhir yaitu proses verifikasi, verifikasi dilakukan dengan cara membandingkan *message digest* dari dokumen berformat *docx* yang telah diinputkan sebelumnya dengan hasil dekripsi dari tanda tangan digital. Jika hasil verifikasi valid maka dapat disimpulkan bahwa tidak adanya terjadi perubahan dokumen beserta tanda tangan digital, sedangkan apabila hasil verifikasi tidak valid maka kemungkinan dokumen atau tanda tangan digital mengalami perubahan, penambahan ataupun pengurangan isi dokumen dan tanda tangan digital telah dimodifikasi. Hasil verifikasi valid dapat dilihat pada gambar 13.



Gambar 13 Verifikasi dokumen berformat *docx* adalah valid

4. KESIMPULAN

Berdasarkan semua hasil pengujian dan pembahasan mengenai implementasi algoritma RSA pada tanda tangan digital dapat diambil kesimpulan sebagai berikut :

1. Aplikasi tanda tangan digital berhasil melakukan enkripsi pada dokumen sehingga menghasilkan tanda tangan digital.
2. Pembangkitan kunci pada algoritma kriptografi RSA memastikan bahwa hanya pasangan kunci yang digunakan untuk proses enkripsi, yang dapat digunakan pada proses dekripsinya.
3. Pengujian penelitian ini memberikan hasil bahwa aplikasi tanda tangan digital menggunakan algoritma kriptografi RSA dapat menjamin keamanan dokumen yang ditandatanganinya dalam aspek *integrity*, *authentication*, dan *non-repudiation*.

5. SARAN

Beberapa saran dari penulis untuk penelitian kedepannyaserta pengembangan aplikasi selanjutnya adalah sebagai berikut :

1. Pengembangan aplikasi yang telah dilakukan masih perlu dilakukan studi, penyesuaian, lebih lanjut seperti penambahan fitur pada pembacaan dokumen.
2. Dapat menggunakan berbagai macam metode ataupun algoritma kriptografi yang lain untuk membuat tanda tangan digital.
3. Dalam pemrosesan Enkripsi dan Dekripsi kunci yang digunakan masih tergolong biasa maka alangkah lebih baik lagi untuk kunci di enkripsikan menggunakan metode yang berbeda.
4. Kunci yang digunakan dalam implementasi masih tergolong lemah karena pendeknya jumlah karakter, maka diharapkan untuk penelitian yang lebih lanjut ada metode pembangkitan karakter.

DAFTAR PUSTAKA

[1] Arief, A. & Saputra, R. 2014. Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging, *Jurnal UNNES Vol 3, No 1*, Universitas Negeri Semarang, Semarang.

[2] Rizaldy, M. R. 2014. Perbandingan Tanda Tangan Digital RSA dan DSA Serta Implementasinya Untuk Antisipasi Pembajakan Perangkat Lunak, *Jurnal Program Studi Teknik Informatika*, Institut Teknologi Bandung, Bandung.

[3] Sulaiman, O. K., Ihwani, M., & Rizki, S.F. 2016. Model Keamanan Informasi Berbasis Tanda Tangan Digital Dengan Data Encryption Standard (DES) Algorithm, *Jurnal InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan) Vol 1, No 1*, Universitas Islam Sumatera Utara, Medan.

[4] Zainuddin, M. A. & Mulyana, D.I. 2016. Penerapan Algoritma RSA Untuk Keamanan Pesan Instan Pada Perangkat Android, *Jurnal CKI On SPOT, Vol. 9, No. 2*, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Jakarta.

[5] Basri. 2016. Kriptografi Simetris dan Asimetris Dalam Perspektif Keamanan Data dan Kompleksitas Komputasi, *Jurnal Ilmiah Ilmu Komputer,* Vol. 2, No. 2, Universitas Al Asyairah Mandar, Sulawesi Barat.

[6] Pahrizal & Pratama, D. 2016. Implementasi Algoritma RSA Untuk Pengamanan Data Berbentuk Teks, *Jurnal Pseudocode,* Vol. 3 No. 1, Universitas Muhammadiyah Bengkulu, Bengkulu.

[7] Kridalaksana, A.H., Rangan, A.Y., & Ansharie, A. 2017. Enkripsi Data Audio Menggunakan Metode Kriptografi RSA, *Jurnal Sebatik STIMIK WICIDA*, STMIK Widya Cipta Dharma, Samarinda.

[8] Ginting, A., Isnanto, R.R., & Windasari, I.P. 2015. Implementasi Algoritma Kriptografi RSA Untuk Enkripsi dan Dekripsi Email, *Jurnal Program Studi Sistem Komputer*, Universitas Diponegoro, Semarang.

[9] Refialy, L., Soediyono, E., & Setiawan, A. 2015. Pengamanan Sertifikat Tanah Digital Menggunakan Digital Signature SHA-512 dan RSA, *Jurnal Teknik Informatika dan Sistem Informasi*, *Vol.1, No.3*, Universitas Kristen Satya Wacana, Salatiga.

[10] Rakhman, A.A, & Kurniawan, A.W. 2015. Implementasi Algoritma Kriptografi Rivest Shamir Adleman (Rsa) Dan Vigenere Cipher Pada Gambar Bitmap 8 Bit, *Jurnal Techno.COM, Vol. 14, No. 2, Mei 2015: 122-134*, Universitas Dian Nuswantoro, Semarang.